**IN THE CLAIMS**

1. (currently amended) A data processing apparatus for executing reproduction of a contents data from a memory device or recording of a contents data into said memory device comprising:

an enabling key block distribution key enciphering key enciphered by an enabling key block~~s~~ containing enciphered data of renewal keys on such paths for constituting a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices, wherein said enabling key block also contains data of upper-rank key enciphered via lower-rank key; ~~wherein~~ and

said data processing apparatus further comprises key distribution approval data files containing header data consisting of link count key for designating the number of contents data that should be enciphered by ~~said~~ enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in said enabling key block~~s~~, thereby said key distribution approval data files are stored in said memory device.

2. (original) The data processing apparatus according to Claim 1, wherein

said key distribution approval data files include a contents key enciphering key data obtained by enciphering contents key for enciphering processing of contents by said key enciphering key.

3. (currently amended) The data processing apparatus according to Claim 1, wherein

said data processing apparatus executes to update said link count ~~data~~ key in said key distribution approval data files in correspondence with variation of the number of contents data that is enciphered by enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in the above-cited enabling key blocks.

4. (original) The data processing apparatus according to Claim 1, wherein

said data processing apparatus stores said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device.

5. (original) The data processing apparatus according to Claim 1, wherein

said data processing apparatus stores said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device; and

whenever processing contents data stored in said memory device, said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device, wherein, solely in the case in which said key enciphering key is

identified to be inapplicable, said data processing apparatus reads said key distribution approval data files.

6. (original) The data processing apparatus according to Claim 1, wherein

version of said enabling key block distribution key enciphering key which is enciphered and presented by said enabling key block is subject to a controlling process by way of renewing every version.

7. (original) The data processing apparatus according to Claim 1, wherein

said data processing apparatus enciphers a plurality of leaf-keys by applying a storage key proper to said data processing apparatus and then stores said enciphered leaf-keys in a memory means inside of said data processing apparatus, wherein said leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses.

8. (original) The data processing apparatus according to Claim 1, wherein

a device key block is stored in a memory means of said data processing apparatus, wherein said device key block itself corresponds to an assemblage of enciphered keys comprising mutually different node keys individually enciphered in plural steps on such paths ranging from own leaves to upper-rank keys of said key tree structure based on such leaf-keys provided in correspondence with own leaves among said key tree structure comprising a variety of keys disposed in correspondence with

roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves.

9. (currently amended) A data processing method for executing reproduction of a contents data from a memory device or recording of a contents data into said memory device, said method comprising:

a step for enciphering an enabling key block distribution key enciphering key by an enabling key block~~s~~ containing enciphered data of renewal keys on such paths for constituting a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices, wherein said enabling key block also contains data of upper-rank key enciphered via lower-rank key; and

a step for storing the key distribution approval data files containing header data consisting of link count key for designating the number of contents data that is enciphered by said enciphering keys in said memory device based on said enabling key block distribution key enciphering key.

10. (original) The data processing method according to Claim 9, wherein

said key distribution approval data files include a contents key enciphering key data obtained by enciphering contents key for enciphering processing of contents by said key enciphering key.

11. (currently amended) The data processing method according to Claim 9, wherein

said data processing apparatus executes to update said link count ~~data~~ key in said key distribution approval data files in correspondence with variation of the number of contents data that is enciphered by enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in the above-cited enabling key blocks.

12. (original) The data processing method according to Claim 9, wherein

said data processing apparatus stores said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device.

13. (original) The data processing method according to Claim 9, wherein

said key enciphering key is stored in said memory, wherein said key enciphering key is acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device; and

whenever processing contents data stored in said memory device, said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device, wherein, solely in the case in which said key enciphering key is

identified to be inapplicable, said data processing apparatus reads said key distribution approval data files.

14. (original) A program providing medium which provides such a computer program to enable a computer system to execute a data processing process via reproduction of a contents data from a memory device or via recording of a contents data into a memory device, said process comprising:

a step for storing said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device; and

a step for executing reading said key distribution approval data files solely in the case where said key enciphering key is identified to be inapplicable, wherein said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device.

15. (previously presented) Apparatus comprising:

a memory device; and

a device for recording data to, or reproducing data from, the memory device, wherein the device stores an enabling key block distribution authenticating key, wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in

correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the device is associated with one of the leaf keys, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys; and

wherein, the memory device stores a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key.

16. (previously presented) The apparatus according to claim 15, wherein the key distribution approval data file comprises a contents key enciphering key (E (KEK, Kcon)) comprising a contents data enciphering contents key (Kcon) enciphered by the key enciphering key (KEK).

17. (previously presented) The apparatus according to claim 15, wherein the memory device updates the link count key in correspondence with a variation in the number of contents data.

18. (previously presented) The apparatus according to claim 15, wherein the memory device stores a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in a key distribution approval data file having a greater count number value for the link-count key than other key distribution approval data files stored in the memory device.

19. (previously presented) The apparatus according to claim 15, wherein the memory device stores a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in

a key distribution approval data file having a greater count number value for the link-count key than other key distribution approval data files stored in the memory device, and wherein the device uses the key enciphering key if it is applicable to the contents data and the other key distribution approval data files otherwise.

20. (currently amended) The apparatus according to claim 15, wherein the ~~wherein the~~ enabling key block distribution authenticating key enciphered by the enabling key block is subject to a version controlling process by way of executing a process for renewing individual versions on the device.

21. (previously presented) The apparatus according to claim 15, wherein the device enciphers a plurality of the leaf keys and then stores the enciphered leaf keys in a memory of the device.

22. (previously presented) The apparatus according to claim 15, wherein the device further comprises a memory for storing a device key block, and wherein the device key block corresponds to an assemblage of enciphered keys comprising mutually different node keys, of the key tree structure, that are individually enciphered.

23. (previously presented) A method for use in recording data to, or reproducing data from, a memory device, the method comprising the steps of:

enciphering an enabling key block distribution authenticating key by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the

key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein a device is associated with one of the leaf keys, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys; and

storing, in the memory device, a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key.

24. (currently amended) The method of claim 23, wherein ~~wherein~~ the key distribution approval data file comprises a contents key enciphering key (E (KEK, Kcon)) comprising a contents data enciphering contents key (Kcon) enciphered by the key enciphering key (KEK).

25. (previously presented) The method of claim 23 further comprising the step of updating the link count key in correspondence with a variation in the number of contents data.

26. (previously presented) The method of claim 23 further comprising the step of storing a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in a key distribution approval data file having a greater count number value for the link-count key than other key distribution approval data files stored in the memory device.

27. (previously presented) The method of claim 23 further comprising the steps of:

storing a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block

distribution authenticating key contained in a key distribution approval data file having a greater count number value for the link-count key than other key distribution approval data files stored in the memory device, and

using the key enciphering key if it is applicable to the contents data and using the other key distribution approval data files otherwise.

28. (previously presented) A computer-readable medium for storing computer-executable software code for the execution of the recording of data to, or the reproduction of data from, a memory device, said code comprising:

code for enciphering an enabling key block distribution authenticating key by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein a device is associated with one of the leaf keys, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys; and

code for storing, in the memory device, a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key.